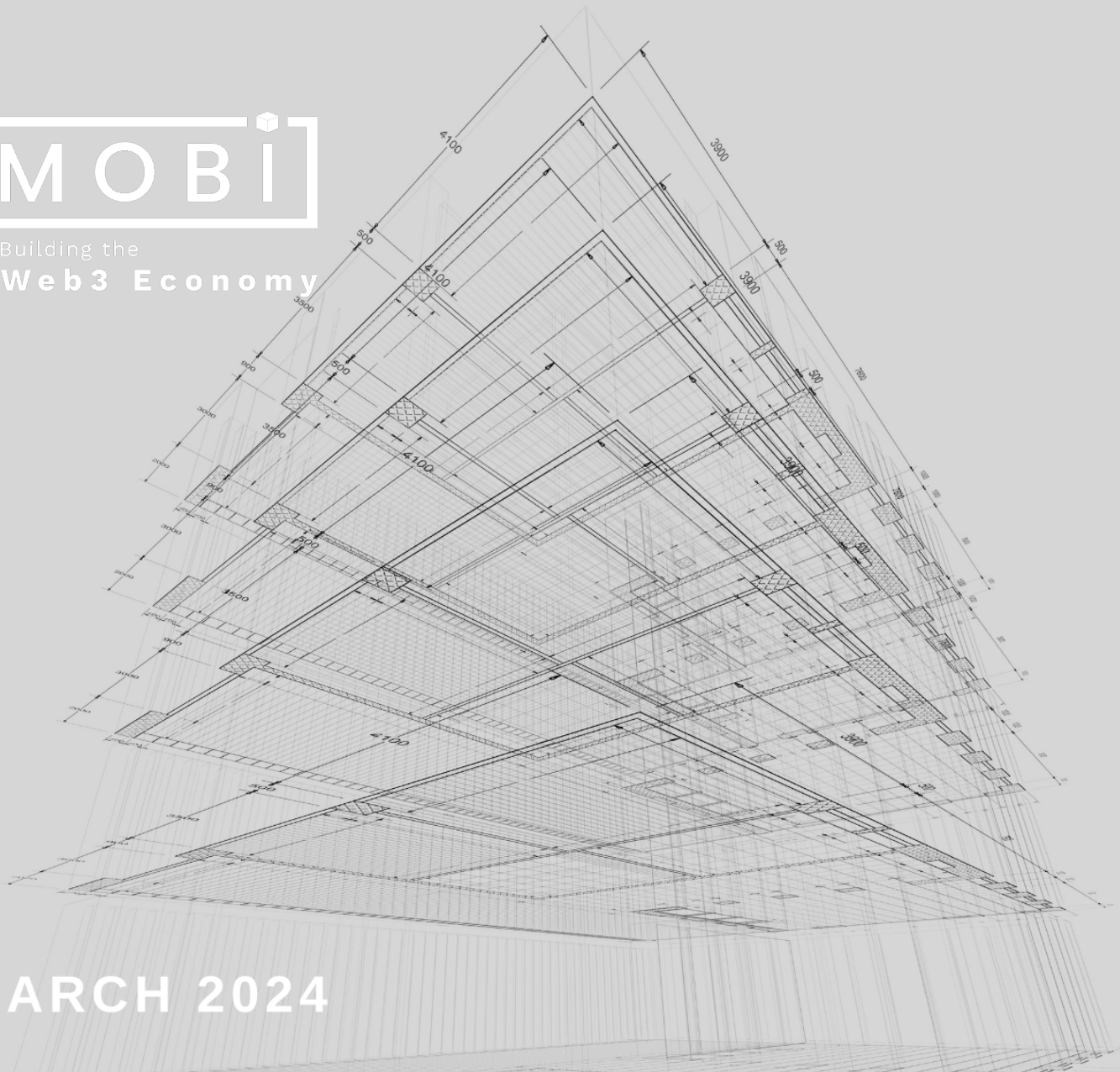




Building the  
Web3 Economy



MARCH 2024

# VEHICLE IDENTITY I TECHNICAL SPECIFICATIONS

MOBI VID0002/TS/2019 Version 2.0

Vehicle Identity (VID) Working Group

© 2024 MOBI. ALL RIGHTS RESERVED.

# TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

© 2024 MOBI

## 1. Definitions.

“**License**” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

“**Licensor**” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

“**Legal Entity**” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

“**You**” (or “**Your**”) shall mean an individual or Legal Entity exercising permissions granted by this License.

“**Source**” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

“**Object**” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

“**Work**” shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

“**Derivative Works**” shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

“**Contribution**” shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.”

“**Contributor**” shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

**2. Grant of Copyright License.** Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

**3. Grant of Patent License.** Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted.

If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

**4. Redistribution.** You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

- a. You must give any other recipients of the Work or Derivative Works a copy of this License; and
- b. You must cause any modified files to carry prominent notices stating that You changed the files; and
- c. You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
- d. If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

**5. Submission of Contributions.** Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

**6. Trademarks.** This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

**7. Disclaimer of Warranty.** Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

**8. Limitation of Liability.** In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

**9. Accepting Warranty or Additional Liability.** While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

Licensed under the Apache License, Version 2.0 (the "License"). You may not use this file except in compliance with the License.

**END OF TERMS AND CONDITIONS**

# INTRODUCTION

This standard was issued by MOBI and its members. MOBI is a nonprofit alliance of many of the world's largest vehicle manufacturers, startups, governments/transit agencies, NGOs, financial institutions, e-mobility providers, consultancies, suppliers, logistics providers, and more working to create standards and build the Web3 digital infrastructure for connected ecosystems and IoT commerce.

MOBI is creating standards for trusted self-sovereign data and identities (e.g. vehicles, people, businesses, things), verifiable credentials, and cross-industry interoperability, with the goal of making transportation more efficient, equitable, decentralized, and circular, all while preserving the data privacy of users and providers alike. MOBI is technology and ledger agnostic. The work of preparing standards is carried out through MOBI Working Groups. Each member of the consortium interested in a subject for which a Working Group has been established has the right to be represented and participate in that Working Group.

The procedures used to develop this document and those intended for its further maintenance are described in the working group charter. In particular, the different approval criteria needed for the different types of MOBI documents should be noted. Approvals of MOBI Steering Committee and Board of Directors are obtained upon the final document release. Attention is drawn to the possibility that some of the elements of this document may be the subject of intellectual property rights. In accordance with MOBI IPLR policy, a 60-day review period is provided to the MOBI community to disclose any and all IP matters pertaining to this standard. MOBI shall not be held responsible for identifying any or all such rights. Details of any IP rights identified during the development of the document will be in the Introduction upon public release of this standard.

Any trade name used in this document is provided for the convenience of users and does not constitute an endorsement. The Working Group responsible for this document is the Vehicle Identity I (VID I) Working Group. Sincere thanks and appreciation are extended to those who contributed their unique insights to the VID I Technical Specifications.

## CONTACT

[connect@dlt.mobi](mailto:connect@dlt.mobi)  
[www.dlt.mobi](http://www.dlt.mobi)

## AUTHORS

Griffin Haskins, MOBI  
Rajat Rajbhandari, MOBI

Andreas Freund, MOBI  
Sid Masih, MOBI

## WG CO-CHAIRS

Sebastien Henot, Renault Group

Alan Gordon, Ford

## CONTRIBUTORS

Praveen Abbaraju, Hitachi  
Steve Amancha, State Farm  
Mark Anders, Ford  
Hiromasa Aoki, TradeLog  
Alessandro Arciero, Henshin Group  
Mitsuharu Arinori, TradeLog  
Murad Baig, Netsoltech  
Sebastian Banescu, Quantstamp  
Joe Bannon, KAR Auction Services  
Patrick Bartsch, AWS  
Brian Behlendorf, Hyperledger Foundation  
Massimo Belluz, Henshin Group  
Roger Berg, DENSO  
Bill Brewster, Olinda Solutions  
Peter Busch, Trusted IoT Alliance  
Lucie Chabert, Stellantis  
Alex Choo, ASJade  
Nicola Cianci, Stellantis  
Etienne Costet, Stellantis  
Michelle Corson, On The Road Lending  
Claudia Damari, Henshin Group  
Daisuke Date, Mazda  
Pierre Delaunay, Stellantis  
Martin Derka, Quantstamp  
Steven Douglas, DENSO  
Olivier Emsalem, Stellantis  
Aaron Fong, Honda  
Daniel Fox, Olinda Solutions  
David Freeman, DLT Labs  
Masahiro Fujita, TradeLog  
Sanshiro Fukao, ITOCHU  
Matteo Gandolfi, Henshin Group  
Fabrizio Garetto, Stellantis  
Todd Gehrke, Luxoft  
John Gerryts, Oaken Innovations  
Alan Gordon, Ford  
Shigemitsu Hara, Orico  
Kawanishi Hiromi, Mazda  
Kinoshita Hiroshi, Mazda  
Max Huang, Celebri AI  
Haolun Huang, DENSO

Tooru Inoue, Orico  
Alvin Ishiguro, TradeLog  
Hitoshi Iwamoto, Honda  
Divyesh Jadav, IBM  
Nick James, AWS  
Sajit Janardhanan, AWS  
Matthew Jones, IBM  
Kazuya Kamata, TradeLog  
Motohisa Kamijo, Nissan  
Masaru Kakuchi, Orico  
Yoji Kawanishi, ITOCHU  
Toru Kimura, Honda  
Christian Koebel, Honda  
Yasuhiro Komine, Honda  
Karthik Krishnamurthy, AWS  
Audrius Kucinskas, CarVertical  
Jignesh Kumar, DENSO  
Subrata Kundu, Hitachi  
Frederic Legrand, Stellantis  
Chengnian Long, CPChain  
Phebe Lu, ASJade  
Kanishk Mahajan, Accenture  
Ishii Makoto, Mazda  
Domenico Mangiacapra, Henshin Group  
Jim Mason, DMX  
Hisashi Matsumoto, Anritsu  
Eiji Matsumura, Anritsu  
Lowell McComb, BMW  
Richard Meszaros, Accenture  
Takuya Mimori, Vitesco  
Emmanuel Monzies, Stellantis  
Takumi Mori, Hioki  
Ryosuke Morisada, Mazda  
Tsunehiko Murai, Orico  
Hiroaki Murase, ITOCHU  
Ash Naik, AAIS  
Hiroshi Nakajima, Orico  
Yasuhiro Nakayama, AUCNET  
Taro Nakata, Kaula Lab  
Alberto Nasi, Stellantis  
Andrea Neri, Stellantis

Keisuke Nisugi, TICO  
Matsuo Naoya, TradeLog  
Takehisa Obara, Hioki  
Yasuhiko Ogushi, Kaula Lab  
Shuichi Ohki, Kaula Lab  
Harunobu Ohmae, ITOCHU  
Katsuji Okamoto, Kaula Lab  
Mitsuyuki Okano, Orico  
Adewale Omoniyi, AWS  
Sunil Paul, SpringFreeEV  
Francesco Petrignani, Traent  
Boris Polania, Honda  
Christian Poulain, Stellantis  
Nick Pudar, GM  
Mathias Reinhartz, Stellantis  
Sandeep Saini, Vitesco  
Futoki Saito, ITOCHU  
Yoshihide Sakai, ITOCHU  
Davide Salerno, Henshin Group  
Shoki Sato, Orico  
Takashi Sendo, TradeLog  
Fabio Severino, Traent  
Otto Schell, Stellantis  
Vyacheslav Sharipov, Aucnet  
Mark Shih, ASJade  
Kikuchi Shinichi, Mazda  
Arwen Smit, MintBit/MOBI  
Sudha Sriram, Ford

Suresh Sundararaj, Ford  
Srinivasa Sunil, Vitesco  
Yoshinori Suzue, Nissan  
Katsutoshi Yamazaki, Honda  
Yasuhiko Yuasa, Honda  
Priya Tabaddor, Cognizant  
Nobuaki Tabata, Mazda  
Yasuhiro Takabe, Mazda  
Yuhei Takai, ITOCHU  
Takahara Shinji, Mazda  
Tatsuro Takahashi, Mazda  
Tetsuya Takahashi, Hioki  
Leonardo Tapanelli, Stellantis  
Sam Teng, ASJade  
Sajjad Thaika, Accenture  
Vitthal Thamke, Vitesco  
Shinnosuke Tsuboyama, Mazda  
Kaiho Tsuneki, Softbank Drive  
Long Tran, AWS  
Christain Umbach, Xapix  
Hisakazu Usui, Mazda  
Wanda Wang, AIOI Insurance  
Takashi Watanabe, Anritsu  
Spencer White, Ford  
Xin Xu, DENSO  
Kubota Yasuyuki, Mazda  
Xiaoliang Zhu, Hitachi

## **MOBI TEAM**

Tram Vo, CEO + Founder  
Chris Ballinger, Advisor + Founder  
Rajat Rajbhandari, Head of Standards & Certification  
Andreas Freund, CTO

Matt Shi, Supply Chain Lead  
Betul Kahya, Mobility Lead  
Parth Bhatt, Technical Product Manager  
Grace Pulliam, Communications Manager

# TABLE OF CONTENTS

About MOBI VID I Tech Specs .....	1
List of Acronyms .....	1
Glossary of Terms .....	2
Objective of this Document .....	5
Scope of MOBI VID Tech Specs .....	5
Typographical Conventions .....	5
General System Requirements .....	6
Certificate Data Format .....	7
Entities .....	13
Bibliography .....	15

## Changelog:

Version	Date Release	Updates
1.0.	07/2019	N/A
1.1.	09/2023	Changed Section 3 title from “System Overview” to “Overview”
2.0.	03/2024	Full rewrite of the Standard, converting it into a concise set of technical requirements. Removed all system-level requirements, making this standard a data specification

## ABOUT MOBI VID | TECH SPECS

---

*The MOBI Vehicle Identity (VID) standard supports advanced mobility use cases like maintenance, insurance, and microtransactions, enabling vehicles to create Self-Sovereign Digital Twins™ for secure, decentralized transactions.*

This document specifies the first standard for MOBI Vehicle Identity (VID), which represents the principal digital foundation of future mobility. The Vehicle Identification Number (VIN), a current vehicle identity system, is insufficient for the digitization of many mobility use cases such as maintenance history, usage-based insurance, microtransactions, and, ultimately, the creation of a vehicle's Self-Sovereign Digital Twin™<sup>1</sup> (a Self-Sovereign Digital Twin™, or SSdT™, is a digital twin that can automatically authenticate its identity and selectively disclose pertinent data for Web3 transactions at the edge without the need to connect to centralized databases). The complete VID and its immutable data can be employed by connected and future autonomous vehicles and the IoT infrastructure that will support them.

The VID is defined as an authoritative form of identity that can be cryptographically verified. Central to this system is a vehicle linked to its unique VID. This VID, established at the vehicle's inception, includes the Vehicle Birth Certificate (VBC) and is indexed by a Unique Vehicle Identifier (UVI). Key stakeholders involved in this system comprise the owner, lien-holder, the original equipment manufacturer (OEM), and government entities, such as Motor Vehicle Authorities (MVAs). Each party may have wallets containing their digital certificates, which unambiguously define their relationship with the vehicle.

*The VID serves as a vehicle's unique identifier, enabling interaction with mobility networks for services like tolls and parking. It uses decentralized identity to authenticate data, allowing owners to monetize shared vehicle data.*

The VID operates as the vehicle's distinctive identifier, facilitating its interaction with various mobility networks. These networks offer services like toll payments, parking, congestion pricing, and more. A key advantage of this connected vehicle ecosystem, compared to traditional methods, is its capacity to authenticate the source and origin of data through the use of decentralized identity and verifiable claims. The data owner has the option to participate in a data marketplace, thereby monetizing the vehicle data they decide to share.

Unlike a centralized architecture where each organization or entity might hold a different perspective of the same vehicle, the decentralized identity-based approach offers an alternative that enables the sharing and regulation of vehicle data, as well as Vehicle-to-Infrastructure (V2I) communication. This method significantly streamlines the intricate, trusted, single-entity systems.

The VID standard is engineered to guarantee that vehicle data can be securely stored within a decentralized environment with access granted only to authorized entities. This facilitates mobility providers in verifying identities, credentials, and related metadata. Consequently, this allows vehicles to establish secure connections with infrastructure, other vehicles, devices, services, and so on.

<sup>1</sup> MOBI. 2023. [dlt.mobi/self-sovereign-digital-twins/](https://dlt.mobi/self-sovereign-digital-twins/).

## LIST OF ACRONYMS

---

CA	:	Certificate Authorities
DID	:	Decentralized Identifier
DLT	:	Distributed Ledger Technology
EID	:	Entity Identifier
ESN	:	Engine Serial Number
OEM	:	Original Equipment Manufacturer
PKI	:	Public Key Infrastructure
P2P	:	Peer-to-Peer
UVI	:	Unique Vehicle Identifier
VBC	:	Vehicle Birth Certificate
VC	:	Verifiable Credential
VID	:	Vehicle Identity
VIN	:	Vehicle Identification Number

## GLOSSARY OF TERMS

---

This section contains the definitions of all technical and specific terms used throughout this document.

**Blockchain:** A blockchain is a growing list of records, called blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a cryptographically secure tree structure such as a Merkle tree.)

**Cryptographically Sound:** A cryptographic method is cryptographically sound if the (cryptographic) statement is false and no cheating prover can convince an honest verifier that it is true (excepting some small probability).

**Decentralized Storage System (DSS):** A DSS is a non-static collection of data storage nodes with a global identifier where each node typically consists of a set of object revisions (“commits”) which each represent a change (creation, update, or deletion) of a single node object. Each commit is signed, immutable, and content-addressable (typically stored and referenced by its hash). The set of commits representing an object is generally append-only, with certain exceptions made, for example, to allow garbage collection of older commits. Objects are associated with a permissioning structure (read/write) controlled by one or more DSS users. The set of data storage nodes utilizes a replication protocol that is deterministic and eventually consistent.

**Decentralized Identifier (DID):** A DID is a globally unique identifier that can be resolved, or de-referenced on a distributed ledger network, much like a URL on the Internet. The DID is resolved to its associated DID Document, which contains the authentication method and service endpoints. A DID can be deactivated. The DID Document also contains cryptographic material, typically in the form of a public-key, that is used to encrypt the payload of all communications to the endpoints. Payload encryption is done independently, and usually in addition to, transport encryption schemas such as SSL or TLS. DIDs can be used with any transport protocol.

**DID Document:** A DID Document is a simple text document that describes how to use that specific DID. Each DID Document may contain at least three things: proof purposes, verification methods, and service endpoints. A DID Document can specify that a particular verification method, such as a cryptographic public key or a pseudonymous biometric protocol, can be used to verify a proof that was created for the purpose of authentication. Service endpoints enable trusted interactions with the DID controller. This document specifies a common data model, format, and operations that all DIDs support.

**Distributed Ledger Technology (DLT):** DLT is a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, or institutions. There is no central administrator or centralized data storage. A peer-to-peer network is required as well as consensus algorithms to ensure replication across nodes is undertaken.

**Entity:** An entity (e.g. vehicle, corporation, individual, etc.) is a network participant that interacts with the system by reading and/or writing data. An entity is identified using an entity certificate (see Section 5.2 Entity Certificate).

**Entity Identifier (EID):** An EID is an unique alphanumeric string that uniquely identifies any entity within the system network described in this document.

**Engine Serial Number (ESN):** The ESN is a unique number that identifies (within the context of a known manufacturer) an engine block.

**Fuel Type:** Type of fuel a vehicle uses (diesel, gasoline, fuel cell, electric, etc.).

**Governance:** Administrator for users, roles and certificate/UVI. On-/Off-boarding of entities is facilitated by the network governance in Section 6.

**Identity:** Identity is a combination of one or more unique identifiers having meta-data associated with them. Identity meta-data consists of certificates such as verifiable credentials (per the W3C definition) and other non-verifiable data objects generated by or on behalf of the unique identifier(s).

**ISO:** International Organization for Standardization

**Motor Vehicle Authority (MVA):** An MVA is an administrative body responsible for overseeing and regulating aspects related to motor vehicles, including licensing, registration, safety standards, and enforcement of related laws and regulations.

**Network:** The system's network is shared equally among network nodes such that no single node (within limits described) may gain an unfair advantage over the overall system.

**Node:** A node on the system network which is maintained by affiliates. A large number of nodes is meant to provide network availability and prevent collusion attacks.

**Original Equipment Manufacturer (OEM):** An OEM is an organization that makes devices from component parts either made internally or sourced from other organizations. In the context of this document, this is synonymous with the vehicle's manufacturer and originator of the vehicle's birth certificate.

**Role:** Roles regulate the creation of and access to data contained within the network.

**Secure Sockets Layer (SSL):** SSL is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.

**Transport Layer Security (TLS):** The TLS protocol is the successor of SSL and aims primarily to provide privacy and data integrity between two or more communicating computer applications.

**Trust Anchor:** A trust anchor is an authoritative entity that validates and qualifies entities on the network specific to the entity's corresponding role.

**Transmission Serial Number (TSN):** The TSN is a unique number that identifies (within the context of a known manufacturer), a transmission unit.

**Uniform Resource Identifier (URI):** URIs ensure that a named URI will always point to the same resource it was assigned to. Note that this is similar to the addressing system on many blockchain platforms and represents one way to implement a URI.

**Unique Vehicle Identifier (UVI):** A UVI is a distinct alphanumeric code within a specific system, differing from a Vehicle Identifier (VID). It acts as a specialized DID for vehicles, linking uniquely to a particular vehicle through its associated Verifiable Credential (VBC), representing the vehicle's minimum digital identity. The UVI facilitates various functions such as verifying existence, controlling access, and confirming specifications. In a simplified view, the UVI serves as a key in a key-value store, allowing for the retrieval of vehicle data from an OEM's network.

**Vehicle Birth Certificate (VBC):** A VBC is a data structure of strings and integers that records information about a particular vehicle at its creation. See Section 4.2 Vehicle Birth Certificate (VBC) for definition and more details.

**Vehicle Identity (VID):** A VID is defined by the verifiable credential adhering to this VID specification issued by the manufacturer as identified by its entity certificate and associated DID.

**Vehicle Identification Number (VIN):** A VIN is a structured combination of characters assigned to a vehicle by the manufacturer for identification purposes.

## OBJECTIVE OF THIS DOCUMENT

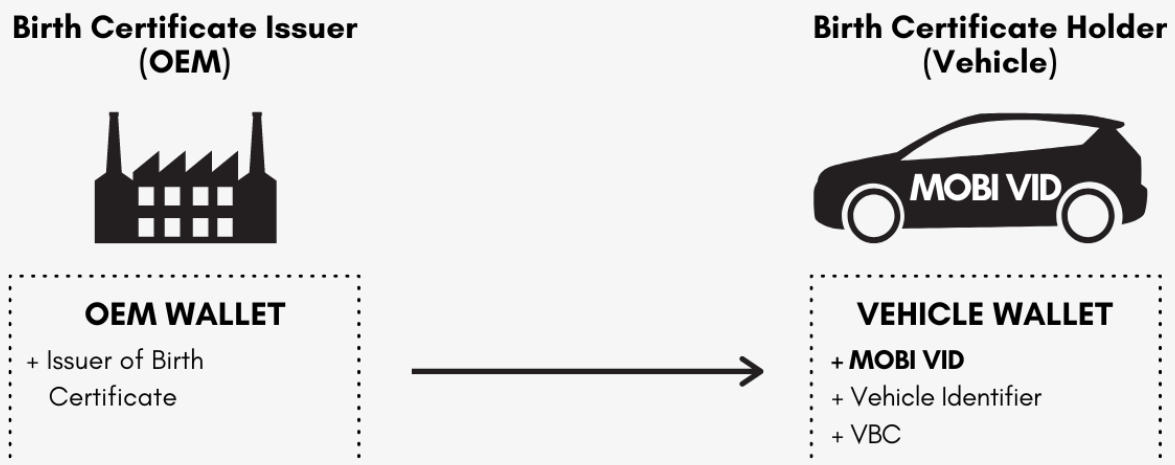
The objectives of this technical specification are to:

- » List out the requirements for implementation of a self-sovereign vehicle identity.
- » Introduce Unique Vehicle Identifier and Vehicle Birth Certificate and provide the data schema.

## SCOPE OF MOBI VID TECH SPECS

*The VID I Technical Specifications outline methods to implement decentralized vehicle identification using W3C standards, focusing on the vehicle birth event and its data structure.*

The VID I Technical Specifications specify the methods and requirements to implement a decentralized vehicle identification system utilizing World Wide Web Consortium (W3C) Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) standards. These specifications focus solely on the vehicle birth event, as depicted in Figure 1. This birth event along with the data structure and all required technical details are described within this document.



**Figure 1.** VID Standard, Initial Release Scope (Vehicle Birth). NOTE: The “Wallet” can be implemented using different methods, including as a Citopia Passport.

## TYPOGRAPHICAL CONVENTIONS

### Requirement IDs

A requirement is identified by a unique ID composed of its requirement level followed by a requirement number, as per the following convention:

[RequirementLevel-RequirementNumber]

Note that requirements are uniquely numbered in ascending order within each requirement level. Four requirement levels are coded in requirement IDs as per the following convention:

[R] - The requirement level for requirements whose IDs start with the letter R is to be interpreted as MUST as described in RFC2119.

[D] - The requirement level for requirements whose IDs start with the letter D is to be interpreted as SHOULD as described in RFC2119.

[O] - The requirement level for requirements whose IDs start with the letter O is to be interpreted as MAY as described in RFC2119.

It should be read that [R1] is an absolute requirement of the specification whereas [D1] is a recommendation and [O1] is truly optional.

## GENERAL SYSTEM REQUIREMENTS

*The system links each UVI with a VBC (including VIN) and uses distributed ledger nodes to enhance data resilience. W3C-specified DIDs regulate API access to VBC data, managing certificates for vehicles and non-vehicle entities.*

### Overview

The system is designed to associate each UVI with a VBC (which includes a VIN). Each individual distributed ledger network node hosts an indistinguishable portion of the network, which improves the resilience of the information on the distributed ledger against hostile network node behavior. Relationships between users regulate API access privileges to the VBC data contained within the network. Certificates are cataloged by a UVI that indexes vehicle certificate entries. Non-vehicle entities, including corporate entities, as well as individuals, are given unique identifiers per W3C-specified DIDs or federated identities (reference Section 6 for technical details) within the system to manage access and activity within certificates.

### System Security and Identity

**VID-R1:** Vehicle IDs MUST follow the W3C DID standard.

**VID-R2:** A vehicle MUST be assigned a Vehicle ID.

Note1.R2: The primary components of the Identity Subsystem will be a global Key Value (KV) store and cryptographic primitives. These two components will interact to allow any user to retrieve another actor's identity and verify that the identity is trusted.

Note2.R2: The VID schema MAY be implemented in a federated method by simply wrapping the VID and VBCs in an existing verifiable, distributed datastore.

Note3.R2: Although a DID is an identifier, it should not be thought of as an identity. An entity's identity can have many DIDs associated with it.

**VID-D1:** Every entity SHOULD use different DIDs for each relationship.

Note1.D1: This strategy helps prevent correlation across systems and other predatory profiling behavior.

Note2.D1: In the case of a vehicle communicating with a system collecting data, correlation is desired, so long-lived DIDs shared across systems is an acceptable model. This could also be done for UVIs, which are an instance of a DID.

**VID-R3:** A DID, combined with an entity certificate, is required to form an authoritative identity.

Note1.R3: Here, an authoritative identity is a fully instantiated, distinct interacting entity.

## Security Considerations

This section introduces some typical requirements for key management. It covers widely recognized best practices and established cryptographic standards.

**VIDI-R4:** All cryptographic services utilized in a VID system MUST be cryptographically sound.

**VID-D2:** Lifecycle management for cryptographic materials generation, exchange, and distribution for use in a VID system SHOULD follow industry best practices such as those outlined in NIST SP 800-57, ISO/IEC 11770, or equivalent thereof.

**VID-D3:** Key management SHOULD follow security best practices as defined in FIPS 200, ISO/IEC 27001, or equivalent thereof.

## Addressing and Uniform Resource Identifiers

**Overview:** Uniform Resource Identifiers (URIs) ensure that a named URI will always point to the same resource it was assigned to.

**VID-R5:** All URIs MUST have a max length of 1024 characters.

# CERTIFICATE DATA FORMAT

In the context of this standard, the minimum viable VID consists of the UVI and its associated VBC. In the following sections, these two key components of VID are described in more detail.

## Unique Vehicle Identifier (UVI)

The UVI (distinct from the VID), is a unique alphanumeric string that is verifiably mapped to a specific vehicle through its associated VBC. This is a minimum representation of that vehicle's digital identity. It can be used to establish existence, enable access control, confirm product specifications, etc. If we abstract the view of the system to a key-value store, then the UVI is the key.

**VID-R6:** The UVI MUST be compliant with the JSON-LD 1.1 schema below:

```
[
  {
    "@context": "http://schema.org",
    "@type": "Unique Vehicle Identifier",
    "attributes": [
      {
        "name": "UVI",
        "description": "Unique Vehicle Identifier, a 64 character alphanumeric string used to uniquely identify a vehicle.",
        "mandatory": "Y",
        "dataStructure": "TEXT UTF8",
        "standardized": "64 character alphanumeric string"
      }
    ]
  }
]
```

Note1.R6: The UVI is validated through the signature of an issuer (entity). The entity itself can be identified through its authoritative identity complaint with the W3C VC specification

## Vehicle Birth Certificate (VBC)

In the abstract view of the system as a KV store, the VBC is a value associated with the UVI. It contains multiple fields including the VIN, manufacturer, model, model year, etc. Some of these fields are intentionally provided for redundancy with respect to the VIN. This adds ease of usability to this VID standard.

**VID-D4:** The Vehicle Birth Certificate SHOULD be compliant with the JSON-LD 1.1 schema below:

```
[
  {
    "@context": "http://schema.org",
    "@type": "Vehicle Birth Certificate",
    "attributes": [
      {
        "name": "Certificate URI",
        "description": "A URI for the Vehicle Birth Certificate.",
        "mandatory": "Y",
        "dataStructure": "URI",
        "standardized": "NOT STANDARDIZED"
      },
      {
        "name": "Color (OEM code)",
        "description": "The color of the vehicle, according to the OEM code.",
        "mandatory": "Y",
        "dataStructure": "TEXT UTF8",
        "standardized": "NOT STANDARDIZED"
      },
      {
        "name": "Country of Origin",
        "description": "The country where the vehicle was manufactured, as per ISO 3779
World Manufacturer Identifier standard.",
        "mandatory": "Y",
        "dataStructure": "TEXT UTF8",
        "standardized": "ISO 3779 WMI"
      },
      {
        "name": "Date of Production",
        "description": "The date when the vehicle was manufactured, represented as a
Linux timestamp.",
        "mandatory": "Y",
        "dataStructure": "LINUX TIMESTAMP",
        "standardized": "RFC 3339/ ISO8601"
      },
      {
        "name": "Engine Code",
        "description": "The code identifying the engine installed in the vehicle, as per
ISO 3779 Vehicle Descriptor Section standard.",
        "mandatory": "Y",
        "dataStructure": "TEXT UTF8",
        "standardized": "ISO 3779 VDS"
      },
      {
        "name": "Engine Serial Number",
        "description": "The unique serial number of the engine installed in the vehicle.",

```

```

        "mandatory": "Y",
        "dataStructure": "TEXT UTF8",
        "standardized": "NOT STANDARDIZED"
    },
    {
        "name": "Fuel Type",
        "description": "The type of fuel used by the vehicle.",
        "mandatory": "Y",
        "dataStructure": "ENUM",
        "standardized": "NOT STANDARDIZED"
    },
    {
        "name": "Manufacturer",
        "description": "The manufacturer of the vehicle, as per ISO 3779 World Manufacturer Identifier standard.",
        "mandatory": "Y",
        "dataStructure": "TEXT UTF8",
        "standardized": "ISO 3779 WMI"
    },
    {
        "name": "Model",
        "description": "The model of the vehicle, as per ISO 3779 Vehicle Descriptor Section standard.",
        "mandatory": "Y",
        "dataStructure": "TEXT UTF8",
        "standardized": "ISO 3779 VDS"
    },
    {
        "name": "Model Year",
        "description": "The year of the model of the vehicle, as per ISO 3779 Vehicle Identifier Section standard.",
        "mandatory": "Y",
        "dataStructure": "TEXT UTF8",
        "standardized": "ISO 3779 VIS"
    },
    {
        "name": "Plant Code",
        "description": "The code identifying the manufacturing plant where the vehicle was produced, as per ISO 3779 World Manufacturer Identifier standard.",
        "mandatory": "N",
        "dataStructure": "TEXT UTF8",
        "standardized": "ISO 3779 WMI"
    },
    {
        "name": "Previous VBC",
        "description": "A link to the previous Vehicle Birth Certificate, if applicable.",
        "mandatory": "N",
        "dataStructure": "URI",
        "standardized": "NOT STANDARDIZED"
    },

```

```

    {
      "name": "Transmission Serial Number",
      "description": "The unique serial number of the transmission installed in the
vehicle.",
      "mandatory": "Y",
      "dataStructure": "TEXT UTF8",
      "standardized": "NOT STANDARDIZED"
    },
    {
      "name": "Trim Type",
      "description": "The type of trim of the vehicle.",
      "mandatory": "Y",
      "dataStructure": "TEXT UTF8",
      "standardized": "NOT STANDARDIZED"
    },
    {
      "name": "UVI",
      "description": "Unique Vehicle Identifier, a 64 character alphanumeric string used
to uniquely identify a vehicle.",
      "mandatory": "Y",
      "dataStructure": "TEXT UTF8",
      "standardized": "64 character alphanumeric string"
    },
    {
      "name": "VIN",
      "description": "Vehicle Identification Number, as per ISO 3779:2009 Content and
Structure standard.",
      "mandatory": "Y",
      "dataStructure": "TEXT UTF8",
      "standardized": "ISO 3779:2009 Content and Structure"
    },
    {
      "name": "Electric Motor Serial Number",
      "description": "The unique serial number of the electric motor installed in the
vehicle, if applicable.",
      "mandatory": "N",
      "dataStructure": "STRING UTF",
      "standardized": "NOT STANDARDIZED"
    },
    {
      "name": "Battery ID",
      "description": "The unique identifier of the battery installed in the vehicle,
if applicable.",
      "mandatory": "N",
      "dataStructure": "STRING UTF",
      "standardized": "MOBI BIN"
    },
    {
      "name": "Battery Installed Date",
      "description": "The date when the battery was installed in the vehicle, if

```

```

applicable.",
    "mandatory": "N",
    "dataStructure": "LINUX_TIMESTAMP",
    "standardized": "NOT_STANDARDIZED"
  },
  {
    "name": "Manufacturer EID",
    "description": "A self-pointer to the EID",
    "mandatory": "Y",
    "dataStructure": "Bytestring",
    "standardized": "W3C DID Protocol"
  }
]
}
]

```

Note1.D4: The following table provides more details regarding some of the fields of the VBC enumerated in the previous subsection.

Term	Description
Date	An unsigned integer indicating the number of milliseconds since midnight of January 1, 1970 UTC (the Linux-Style Timestamp <sup>2</sup> ).
Fuel Type	0 = Petroleum 1 = Diesel 2 = Electric 3 = Hybrid 4 = Fuel Cell 5 = Natural Gas 6 = Other

**VID-R7:** A valid VBC MUST be issued by the legal identity of an Original Equipment Manufacturer (OEM).



<sup>2</sup> <http://man7.org/linux/man-pages/man1/time.1.html>

# ENTITIES

## Overview

Entities form the means of interaction among participants in the network. System participants are represented by entities that also take on specific roles within the systems' role-based permissioning. An entity certificate defines an identity within the system which allows the entity to interact with VBCs through the role permission system.

**VID-D5:** Entity actions MUST be cryptographically authenticated by one of the Verification Methods listed in the verificationMethod data property and referenced in the authentication data property of the DID Document of the DID referred to in the Entity's EID.

## Entity Certificate

An "Entity" in the system can be any network participant, from a government entity to an individual, who wants to interact with a vehicle (Fig. 1). In this context, an entity defines an identity, which consists of an identifier (e.g. W3C-compliant DID) and an associated Entity Certificate (EC).

**VID-R8:** The EC MUST be compliant with the JSON-LD 1.1 schema below:

```
[
  {
    "@context": "http://schema.org",
    "@type": "Entity Certificate",
    "attributes": [
      {
        "name": "EID",
        "description": "A self-pointer to the EID",
        "mandatory": "Y",
        "dataStructure": "Bytestring",
        "standardized": "W3C DID Protocol"
      },
      {
        "name": "Type",
        "description": "Type of Entity, values see below",
        "mandatory": "Y",
        "dataStructure": "Int",
        "standardized": "Not Standardized"
      },
      {
        "name": "PubKey",
        "description": "The public key in the PKI that is used to communicate with this
EID",
```

```

    "mandatory": "Y",
    "dataStructure": "Bytestring",
    "standardized": "TLS 1.3"
  },
  {
    "name": "---",
    "description": "Custom fields",
    "mandatory": "---",
    "dataStructure": "---",
    "standardized": "---"
  }
]
}
]

```

Note1.R8: For the onboarding process, entities may receive a verifiable credential compliant with the W3C DID specification or, alternatively, receive one based on a federated identity provider.

Note2.R8 The “Type” field from above is one of either 1, 2, 3, 4, or 5 with definitions as follows:

- » Users
- » Physical Assets
- » Service Providers
- » Data Hosts
- » Trust Anchors (Government, Consortium, etc.)



<sup>3</sup> [https://en.wikipedia.org/wiki/Federated\\_identity#Examples](https://en.wikipedia.org/wiki/Federated_identity#Examples)

## BIBLIOGRAPHY

---

**Normative References** - The following documents are referenced in such a way that some or all of their content constitutes requirements of this document.

[RFC 2119]

S. Bradner, Key words for use in RFCs to Indicate Requirement Levels,  
<http://www.ietf.org/rfc/rfc2119.txt>, IETF RFC 2119, March 1997.

[RFC 3986]

T. Berners-Lee, R. Fielding, L. Masinter, Uniform Resource Identifier (URI): Generic Syntax,  
<https://datatracker.ietf.org/doc/html/rfc3986>, IETF RFC 3986, January 2005.

[ISO 3779]

ISO, Road vehicles — Vehicle identification number (VIN) — Content and structure,  
<https://www.iso.org/standard/52200.html>, ISO 3779:2009, October 2009.

[RFC 3339]

G. Klyne, C. Newman, Date and Time on the Internet: Timestamps,  
<https://datatracker.ietf.org/doc/html/rfc3339>, IETF RFC 3339, July 2002.

### Non-Normative References

[W3C-DID]

Decentralized Identifiers (DIDs) v1.0, M. Sporny, D. Longley, M. Sabadello, D. Reed, O. Steele, C. Allen, W3C W3C Recommendation, July 2022,  
<https://www.w3.org/TR/2022/REC-did-core-20220719/>. Latest version available at <https://www.w3.org/TR/did-core/>.

[FIPS 200]

National Institute of Standards and Technology, Minimum Security Requirements for Federal Information and Information Systems,  
<https://doi.org/10.6028/NIST.FIPS.200>, FIPS 200, March 2006.

[NIST SP 800-57]

E. Barker, Recommendation for Key Management: Part 1 – General,  
<https://doi.org/10.6028/NIST.SP.800-57pt1r5>, NIST SP 800-57 Part 1 Rev. 5, May 2020.

[ISO/IEC 11770]

ISO/IEC, Information security — Key management — Part 3: Mechanisms using asymmetric techniques,  
<https://www.iso.org/standard/82709.html>, ISO/IEC 11770-3:2021, October 2021.

[ISO/IEC 27001]

ISO/IEC, Information security management systems - Requirements,  
<https://www.iso.org/standard/27001>, ISO/IEC 27001:2022, October 2022.

[JSON-LD 1.1]

JSON-LD 1.1, M. Sporny, D. Longley, G. Kellogg, M. Lanthaler, Pierre-Antoine Champin, N. Lindström, W3C Recommendation, July 2020 ,  
<https://www.w3.org/TR/2020/REC-json-ld11-20200716/>. Latest version available at <https://www.w3.org/TR/json-ld11/>.